National Infrastructure Protection Center
CyberNotes

Issue #2001-18 *September 10, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 22 and September 6, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
AOL[1]	Windows 95/98/ME/ NT 4.0/2000, MacOS 10.x, Unix	AOLserver 3.0, 3.2	A remote Denial of Service vulnerability exists due to the way passwords are handled.	No workaround or patch available at time of publishing.	AOLServer Long Authentication String Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] Bugtraq, August 22, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Baltimore Technol-ogies[2]	Windows NT 4.0	WEB sweeper 4.02	A security vulnerability exists which could let a remote malicious user gain access to known restricted web directories.	Baltimore Technologies has released a technote that suggests that it is not practical to use WEBsweeper to administer URL blacklists. This document is available at: http://www.mimesweeper.com/support/technotes/notes/1043.asp	WEBsweeper Restricted Directory Disclosure	Medium	Bug discussed in newsgroups and websites.
Caldera Interna-tional, Incor-porated[3]	Unix	OpenUnix 8.0	A buffer overflow vulnerability exists in the 'LPSystem' program, which could let a malicious user gain elevated privileges.	Update available at: ftp://ftp.sco.com/pub/security/openunix/sr847408/erg711789a.Z	Open Unix 'LPSystem' Buffer Overflow	Medium	Bug discussed in newsgroups and websites.
Caldera Interna-tional, Incor-porated[4]	Unix	UnixWare 7, OpenUnix 8.0	A buffer overflow vulnerability exists in 'UIDAdmin', which could let a malicious user gain root access.	Patch available at: ftp://ftp.sco.com/pub/security/openunix/sr847563/erg711722a.Z	Open Unix 'UIDAdmin' Scheme Option Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Carnegie Mellon University[5]	Unix	Cyrus 1.6.24	A Denial of Service vulnerability exists when running under BSDi 4.2 using PHP's IMAP functionality.	No workaround or patch available at time of publishing.	Cyrus IMAP Server Potential Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[6]	Multiple	CBOS 2.0.1, 2.1.0, 2.1.0a, 2.2.0, 2.2.1, 2.2.1a, 2.3, 2.3.2, 2.3.5, 2.3.7, 2.3.8, 2.3.9, 2.4.1, 2.4.2, 2.4.2ap	Multiple Denial of Service vulnerabilities exist in the Cisco Broadband Operating System (CBOS) when it receives multiple TCP connections on one of the two administrative ports: 21 via Telnet, or 80 via HTTP.	Upgrade available at: http://www.cisco.com/	Cisco CBOS Multiple TCP Connection Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
FreeBSD, Incor-porated[7]	Unix	FreeBSD 4.1.1-RELEASE, 4.2-RELEASE, 4.3-RELEASE	A vulnerability exists in tcp_wrappers that may cause some checks to fail when the 'PARANOID' ACL option is enabled in the configuration file, which could let a remote malicious user bypass the host access control rules.	Patch available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:56/tcp_wrappers.patch	FreeBSD tcp_wrappers 'PARANOID' Checking Bypass	Medium	Bug discussed in newsgroups and websites.
FreeBSD, Incor-porated[8]	Unix	FreeBSD 4.2, 4.3	A vulnerability exists in the 'rmuser' script because it temporarily creates a world readable copy of 'master.passwd', which could let a malicious user gain elevated privileges.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-01:59/rmuser.patch	FreeBSD 'rmuser' Password Hash Disclosure	Medium	Bug discussed in newsgroups and websites.

[2] Securiteam, September 6, 2001.
[3] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.15, August 28, 2001.
[4] Caldera International, Inc. Security Advisory, CSSA-2001-SCO.14, August 23, 2001.
[5] Bugtraq, August 30, 2001.
[6] Cisco Security Advisory, August 23, 2001.
[7] FreeBSD Security Advisory, FreeBSD-SA-01:56, August 23, 2001.
[8] FreeBSD Security Advisory, FreeBSD-SA-01:59, September 3, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
global SCAPE[9]	Windows 95/98/NT 3.5.1/4.0/ 2000	CuteFTP 4.2	A vulnerability exists because passwords are stored using a weak encryption algorithm, which could let a malicious user gain unauthorized access.	No workaround or patch available at time of publishing.	CuteFTP Weak Password Encoding	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
GMD FIT[10]	Unix	BSCW 3.0-3.4.3	A vulnerability exists in BSCW (Basic Support for Cooperative Work) because symlinks are not properly handled, which could let a malicious user execute arbitrary commands.	Upgrade available at: http://bscw.gmd.de/	BSCW Symbolic Link File Disclosure	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
GNU[11]	Unix	Mailman 2.0-2.0.5	A vulnerability exists when a password file has been created but left blank, which could let a remote malicious user gain access to the account.	**GNU:** ftp://ftp.gnu.org/gnu/mailman/mailman-2.0.6.tgz **Conectiva:** ftp://atualizacoes.conectiva.com.br/	Mailman Empty Password Blank Salt	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company[12]	Unix	HP Process Resource Manager C.01.07, C.01.08.02	A vulnerability exists in the Process Resource Manager (PRM) add-on package, which could let a malicious user gain root access. *Note: Since HP-UX Workload Manager (WLM) uses PRM to control resources, the vulnerability also exists for this software.*	Upgrade available at: PHSS_24864 PHSS_24863 http://itrc.hp.com	HP Process Resource Manager Environment Variable Privilege Elevation	**High**	Bug discussed in newsgroups and websites.
Hewlett Packard Company[13]	Unix	HP-UX 10.26	A vulnerability exists in the login function because unsuccessful login attempts are not recorded in 'btmp', which could let a malicious user launch a brute force attack.	Patch available at: PHCO_17719 http://itrc.hp.com	HP-UX login btmp Logging Failure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard Company[14]	Unix	HP-UX 11.0	A buffer overflow vulnerability exists in the 'SWVerify' program, which could let a malicious user execute arbitrary code and potentially gain administrative access.	Patch available at: PHCO_23483 http://itrc.hp.com	HP-UX 'SWVerify' Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Hewlett Packard Company[15]	Windows NT 4.0	CIFS/9000 Server A.01.05-A.01.07	A vulnerability exists when the "unix password sync" option is enabled. In this case, Samba will attempt to synchronize smbpasswd and unix password by calling the program in the "passwd program" option. If the passwd program string does not include the %u substitution, another user's password can be changed unintentionally during this process and elevated privileges can be gained.	**Workaround:** Customers are advised to check their CIFS configuration files, and ensure the passwd program looks like the following: passwd program = /bin/passwd %u	CIFS 9000 Arbitrary Password Changing	Medium	Bug discussed in newsgroups and websites.

[9] Bugtraq, August 23, 2001.
[10] Securiteam, August 27, 2001.
[11] Conectiva Linux Security Announcement, CLA-2001:420, September 5, 2001.
[12] Hewlett-Packard Company Security Bulletin, HPSBUX0108-165, August 29, 2001.
[13] SecurityFocus, September 4, 2001.
[14] Securiteam, September 4, 2001.
[15] Hewlett-Packard Company Security Bulletin, HPSBUX0108-164, August 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett-Packard Company [16]	Unix	HP-UX 10.1, 10.10, 10.20, 11.0, 11.11	A buffer overflow vulnerability exists in the 'rlpdaemon', which could let a remote malicious user execute arbitrary code.	Patches available at: PHCO_24701, PHCO_24700, PHCO_24699, PHCO_24698, PHCO_24697 http://us-support.external.hp.com	HP-UX Line Printer Daemon Buffer Overflow CVE Name: CAN-2001-0668	**High**	Bug discussed in newsgroups and websites.
IBM[17]	Unix	Informix SQL 7.31.UC5	A vulnerability exists in the Informix SQL add-on package due to the creation of a predictable file "snmpd.log" in the /tmp directory, which could let a malicious user create any file with root privilege; and a vulnerability exists in the 'onsrvapd' program, which could let a malicious user overwrite root-owned files, and potentially gain elevated privileges, including root access.	No workaround or patch available at time of publishing.	Informix SQL SNMPDM and ONSRVAPD Predictable Temporary File Creation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
IBM[18]	Unix	Informix SQL 7.31.UC5	A symbolic link vulnerability exists because the programs 'onbar_d', 'ondblog', and 'onsmsync' create predictable files in the /tmp directory, which could let a malicious user gain elevated privileges.	No workaround or patch available at time of publishing.	Informix SQL Temporary Log File Symbolic Link	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
IDM Computer Solutions, Incor-porated[19]	Windows 95/98/NT 3.5/4.0/ 2000	UltraEdit-32 8.2	A vulnerability exists because passwords are stored using a weak encryption algorithm, which could let a malicious user gain unauthorized access.	No workaround or patch available at time of publishing.	UltraEdit FTP Client Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Inter7[20]	Multiple	vpopmail (vchkpw) 3.4.1-4.9.10	A vulnerability exists when vpopmail is configured to use the MySQL database, which could let a malicious user gain sensitive information.	No workaround or patch available at time of publishing.	Vpopmail MySQL Authentication Data Recovery	Medium	Bug discussed in newsgroups and websites.
Kabotie Software Technol-ogies[21]	Multiple	ShopPlus Cart 1.0	A vulnerability exists because certain types of user-supplied input are not filtered, which could let a malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	ShopPlus Cart Arbitrary Command Execution	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[16] Hewlett-Packard Company Security Bulletin, HPSBUX0108-163, August 27, 2001.
[17] Bugtraq, September 4, 2001.
[18] Bugtraq, September 4, 2001.
[19] Bugtraq, August 23, 2001.
[20] BUZ.CH Security Advisory 200109041, September 4, 2001.
[21] Securiteam, September 6, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Marconi Corporation[22]	Multiple	ForeThought 7.2	A Denial of Service vulnerability exists because the Telnet administration interface allows up to two concurrent sessions.	No workaround or patch available at time of publishing.	ForeThought 7.1 Telnet Administration Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[23]	Windows NT 4.0/2000	Exchange 5.5, 5.5SP1-SP4	A vulnerability exists because a function in Outlook Web Access (OWA) that interrogates the global address list (GAL) doesn't require authentication, which could let a malicious user learn the e-mail addresses of users on the server.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-047.asp	Exchange OWA Global Access Information Disclosure CVE Name: CAN-2001-0660	Medium	Bug discussed in newsgroups and websites.
Microsoft[24]	Windows 95/98/ME/ NT 4.0/2000	Outlook Express 6.0	A vulnerability exists that allows a file embedded within an HTML frame in an e-mail message to bypass the file attachment security feature and possibly execute arbitrary programs.	No workaround or patch available at time of publishing.	Outlook Express 6 Attachment Security Bypass	Medium/ **High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Mozilla Project[25]	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.10, 2.12, 2.4, 2.6, 2.8	Input validation vulnerabilities exist in the 'showvotes.cgi', 'createaccount.cgi', and 'reports.cgi' scripts because HTML tags are not stripped from requests, which could let a malicious user submit a malicious link that contains arbitrary script code.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.14.tar.gz	Multiple BugZilla Cross-Site Scripting Vulnerabilities	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Mozilla Project[26]	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.10, 2.12, 2.4, 2.6, 2.8	An input validation vulnerability exists when a remote malicious user submits an arbitrary bug ID number as an argument to 'showattachment.cgi', disclosing sensitive information about "restricted" bugs; and a vulnerability exists in the 'describecomponents.cgi' which could allow a malicious user to obtain sensitive information.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.14.tar.gz	BugZilla 'showattachment.cgi' and 'describecomponents.cgi' Arbitrary Bug Viewing	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[22] Securiteam, September 6, 2001.
[23] Microsoft Security Bulletin, MS01-047, September 6, 2001.
[24] Securiteam, August 31, 2001.
[25] Bugtraq, August 29, 2001.
[26] Bugtraq, August 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla Project [27]	Windows 95/98/NT 3.5.1/4.0	BugZilla 2.10, 2.12, 2.8	Vulnerabilities exist through the 'show_activity.cgi', and 'showdependencytree.cgi', interfaces, which could let a remote malicious user gain sensitive bug information; and a vulnerability exists in that when viewing a restricted bug, the user may save the 'show_bug.cgi' page and modify the hidden form fields. Loading this modified page and clicking 'commit' reveals the hidden comments.	Upgrade available at: http://ftp.mozilla.org/pub/webtools/bugzilla-2.14.tar.gz	Multiple BugZilla Restricted Bug Comment Revealing Vulnerabilities	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[28]	Unix	Network Associates PGP e-ppliance 300 series 1.0, 1.5, 2.0; Gauntlet Firewall for Unix 5.0, 5.5, 6.0; McAfee WebShield for Solaris 4.0	A boundary condition vulnerability exists in the smap/smapd and CSMAPD daemons, which could let a malicious user execute arbitrary code.	**Network Associates:** ftp://ftp.nai.com/pub/security/ **McAfee:** www.mcafeeb2b.com	Gauntlet Firewall for Unix and WebShield CSMAP and smap/smapd Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[29]	Unix	OpenBSD 2.0-2.9; NetBSD 1.0-1.5.1; FreeBSD 2.2-4.2'; BSDI BSD/OS 2.0-4.1	A buffer overflow vulnerability exists in the BSD print protocol daemon, which could let a remote malicious user gain superuser access.	**BSDI BSD/OS:** http://www.BSDI.COM/services/support/patches/patches-4.1/M410-044 **FreeBSD:** ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/SA-01:58/lpd-3.x-4.2.patch	Multiple BSD Vendor lpd Buffer Overflow CVE Name: CAN-2001-0670	**High**	Bug discussed in newsgroups and websites.

[27] Bugtraq, August 29, 2001.
[28] PGP Security Advisory, September 4, 2001.
[29] Internet Security Systems Security Advisory, ISS-094, August 29, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[30]	Unix	Vivek Khera mod_auth_mysql 1.9; Min S. Kim AuthPG 1.2b2; Serg Oskin mod_auth_oracle 0.5.1; Guiseppe Tanzilli, Matthias Eckermann, and Victor G mod_auth_pgsql_sys 0.9.4; Guiseppe Tanzilli and Matthias Eckermann mod_auth_pgsql 0.9.5	Vulnerabilities exists in the 'mod_auth_mysql' (Vivek Khera), 'AuthPG' (Min S. Kim), 'mod_auth_oracle' (Serg Oskin), 'mod_auth_pgsql' (Guiseppe Tanzilli, Matthias Eckermann, and Victor G), and 'mod_auth_pgsql_sys' (Guiseppe Tanzilli and Matthias Eckermann) authentication modules, which will allow SQL queries to be manipulated via a HTTP request. This could let a remote malicious user execute arbitrary SQL statements or cause the database query for the password to return arbitrary data.	Update available at: **Vivek Khera:** ftp://ftp.kcilink.com/pub/ **Min S. Kim:** http://authpg.sourceforge.net/ **Serg Oskin:** The vendor has announced that a fixed version is forthcoming. **Guiseppe Tanzilli and Matthias Eckermann**: mod_auth_pgsql 0.9.5: http://www.giuseppetanzilli.it/mod_auth_pgsql/dist/	Multiple Apache Remote SQL Query Manipulation Vulnerabilities	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Multiple Vendors[31, 32, 33]	Unix	Xinetd 2.1.8.8, 2.1.8.8pre3, 2.1.8.9pre1-2.1.8.9pre15, 2.1.8.9pre2, 2.1.8.9pre3, 2.1.8.9pre5-2.1.8.9pre9, 2.3	Multiple security vulnerabilities exist, which could let a remote malicious user cause a Denial of Service or a root compromise.	**Xinetd:** http://www.xinetd.org/xinetd-2.3.3.tar.gz **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Immunix:** http://download.immunix.org/ImmunixOS/7.0/updates/RPMS/ **MandrakeSoft:** ftp://ftp.cadvision.com/pub/linux/Mandrake/Mandrake/updates/	Multiple Xinetd	Low/**High**	Bug discussed in newsgroups and websites.

[30] RUS-CERT Advisory 2001-08:01, August 29, 2001.
[31] Conectiva Linux Security Announcement, CLA-2001:416, August 29, 2001.
[32] Immunix OS Security Advisory, IMNX-2001-70-033-01, August 29, 2001.
[33] Mandrake Linux Security Update Advisory, MDKSA-2001:076, August 31, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[34]	Windows NT 4.0/2000	Cisco Secure IDS Host Sensor 2.0, IDS Network Sensor 3.0, 6000 IDS Module; Internet Security Systems BlackIce Agent 2.5, 3.0, BlackIce Sentry 2.5, 3.0, BlackIce Guard 2.5, BlackIce Defender 2.5, 2.5cg; Internet Security Systems RealSecure Server Sensor 5.0 Win, 5.5 Win, 5.5.1 Win, 5.5.2 Win, 6.0 Win, 5.0, 5.5, 5.5.1, 5.5.2, 6.0; Martin Roesch Snort 1.5, 1.5.1, 1.5.2, 1.6, 1.6.1, 1.6.2, 1.6.3, 1.7, 1.8; NFR Network Intrusion Detection 5.0	A vulnerability exists in the way many Intrusion Detection Systems (IDS) handle parsing of Unicode HTTP encoded requests (%xxxx), which could let a remote malicious user to attack applications such as web servers while avoiding detection by the IDS.	Contact your vendor for upgrade.	Multiple IDS Vendor Encoded IIS Attack Detection Evasion CVE Name: CAN-2001-0669	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
NetBSD[35]	Unix	NetBSD current pre20010805 1.4-1.5.1	An input validation vulnerability exists due to insufficient length checking on a parameter passed to the 'semop()' function, which could let a malicious user cause a Denial of Service and/or execute arbitrary code and gain root privileges.	Update available at: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2001-015-kernlen-1.5.patch	NetBSD 'semop' Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites.

[34] Internet Security Systems Security Alert, September 5, 2001.
[35] NetBSD Security Advisory, 2001-015, September 5, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetBSD[36]	Unix	NetBSD current pre20010805 1.4-1.5.1	A Denial of Service vulnerability exists due to an input validation error in the 'ioctl(9)' routines provided by several drivers included in the kernel.	Update available at: ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2001-015-kernlen-1.5.patch	NetBSD 'ioctl' Denial of Service	Low	Bug discussed in newsgroups and websites.
Netscape Communi-cations[37]	Unix	Communi-cator 6.01a	A symlink vulnerability exists because insecure temporary files are created when installed on Solaris systems, which could let a malicious user overwrite sensitive system files.	No workaround or patch available at time of publishing.	Communicator Temp File Symbolic Link	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Network Associates [38]	Windows 95/98/ME/ NT 4.0/2000, MacOS 9.0, OS/390 V2R9, OS/390 V2R6, Unix	PGP Personal Security 7.0.3; PGP Freeware 7.0.3; PGP E-Business Server 6.5.8, 7.0.4, 7.1; PGP Corporate Desktop 7.1; PGP 5.0, 6.0.2	A vulnerability exists in some of PGP's display of key validity, which could allow a malicious user to trick others into accepting a key associated with an invalid user ID.	Patch available at: http://download.nai.com/products/licensed/pgp/	PGP Invalid Key Display	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
PHPMy Explorer[39]	Unix	MyExplorer Classic 1.0-1.1.0, 1.1.3-1.1.5, 1.2; MultiUser 1.0	An input validation vulnerability exists, which could let a malicious user obtain sensitive information.	Upgrade available at: http://elegac.free.fr/commun/download/phpmonexplorateur1.2.1install_(php3).zip	MyExplorer Arbitrary File Disclosure	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
PHPProjekt Develop-ment Team[40]	Windows NT 4.0/2000, Unix	PHPProjekt 2.0-2.4	An input validation vulnerability exists, which could let a remote malicious user obtain elevated privileges.	Upgrade available at: http://www.phprojekt.com/download.html	PHPProjekt Arbitrary User Modification	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
POP3Lite[41]	Unix	POP3Lite 0.2.3, 0.2.3b	An input validation vulnerability exists because leading dots ('.') are not escaped from e-mail transfers, which could let a remote malicious user pass arbitrary server responses embedded in carefully crafted e-mails, possibly leading to arbitrary message injection and lost messages.	Upgrade available at: ftp://pop3lite.sourceforge.net/pub/pop3lite/	POP3Lite Input Validation	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[36] NetBSD Security Advisory, 2001-015, September 5, 2001.
[37] SecurityFocus, August 27, 2001.
[38] Bugtraq, September 4, 2001.
[39] eRisk Security Advisory, August 29, 2001.
[40] Bugtraq, August 26, 2001.
[41] Securiteam, September 4, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Qualcomm, Incor-porated[42]	Unix	qpopper 4.0.1	A vulnerability exists when qpopper is used in conjunction with PAM on RedHat Linux systems because different error messages are displayed when authentication attempts are made using valid and invalid usernames, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PAM qpopper User Enumeration	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
RedHat[43]	Unix	Linux 6.2, 7.0, 7.1	On some systems, 'dvips' is not invoked in a safe manner, which could let a remote malicious user execute arbitrary commands through certain DVI directives through 'lpd'.	No workaround or patch available at time of publishing.	Lpd Remote Command Execution via DVI Printfilter Configuration Error	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Respondus [44]	Windows 95/98/NT 4.0/2000	Respondus for WebCT 1.1.2	A vulnerability exists because passwords are stored using a weak encryption algorithm, which could let a malicious user gain unauthorized access.	The vendor has confirmed this issue and a fixed version is forthcoming.	Respondus for WebCT Weak Password Encryption	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Robert Munafo[45]	Windows, Unix	Gnut 0.4.20-0.4.27	A vulnerability exists in the web interface, 'webfrontend', because it allows HTML code to be injected in the search result page, which could let a malicious user embed arbitrary script code in a filename that may be run locally when the file turns up in a search.	Upgrade available at: http://www.gnutelliums.com/linux_unix/gnut/	Gnut Gnutella Client Arbitrary Script Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Starfish Software[46]	Windows	TrueSync Desktop 2.0	Two vulnerabilities exist due to a trivial method of storing user passwords and protected data files are not encrypted, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	TrueSync Desktop Failure to Protect Data and Desktop Password Disclosure	Medium	Bug discussed in newsgroups and websites.
Sun Micro-systems, Incor-porated[47]	Unix	Java 2 Runtime Environment 1.3, Java Plug-In 1.4	A vulnerability exists because users may not be alerted by the plugin/JRE when applets have been signed with expired certificates, which could lead to a user believing that the applet is valid and allow it to be run on the local computer.	Unofficial workaround (SecurityFocus): Ensure that version 1.4 of Plug-In is not installed with JRE 1.3.	Java Plug-In 1.4/JRE 1.3 Expired Certificate	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[42] Bugtraq, August 25, 2001.
[43] SecurityFocus, August 27, 2001.
[44] Bugtraq, August 23, 2001.
[45] Securiteam, September 4, 2001.
[46] Bugtraq, August 24, 2001.
[47] SecurityFocus, August 24, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Incor-porated[48]	Unix	Solaris 2.0-2.3, 2.4-2.6 & 2.4_x86-2.6_x86, 7.0-8.0, 7.0_x86-8.0_x86	A vulnerability exists in the print protocol daemon, 'in.lpd' (or 'lpd'), which could let a remote malicious user execute arbitrary commands with superuser privileges.	Patch available at: http://sunsolve.sun.com/securitypatch	Solaris lpd Remote Command Execution	High	Bug discussed in newsgroups and websites. Exploit script exists but has not been published. It should be assumed that this is being actively exploited 'in the wild.'

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 22 and September 7, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 13 scripts, programs, and net-news messages containing holes or exploits were identified. *At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 7, 2001	Altering_ARP_Tables_v_1.00.htm	This paper is dedicated to ARP tables and how to alter them remotely; it also includes a couple of sample implementations of ARP poisoning.
September 5, 2001	Smsspoof-1.1.tar.gz	An application that allows a person to send spoofed SMS messages with a Palm Pilot.
September 4, 2001	Hp-swverify.c	Script which exploits the HP Process Resource Manager Environment Variable Privilege Elevation vulnerability.

[48] Sun Microsystems, Inc. Security Bulletin #00206, August 30, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
September 3, 2001	Ssh-timing.pdf	A document titled *Timing Analysis of Keystrokes and Timing Attacks on SSH* describes how to obtain information about the contents of a packet by watching the timing between keystrokes sent over SSH and other encrypted protocols..
August 31, 2001	**Ykk.zip**	**Exploit script for the Outlook Express 6 Attachment Security Bypass vulnerability.**
August 28, 2001	Asc.c	An IA 32 Alphanumeric Shellcode Compiler that was published in Phrack 57.
August 28, 2001	Irs10.exe	A Windows NT/2k tool that finds out which network restrictions have been set for a particular service on a host. It combines "ARP Poisoning" and "Half-Scan" techniques and tries totally spoofed TCP connections to the selected port of the target.
August 27, 2001	**Aolcrash.c**	**Script which exploits the AOLServer Long Authentication String Remote Denial of Service vulnerability.**
August 27, 2001	Patchadd.pl	Perl script which exploits the Solaris 2.8 patchadd symlink vulnerability.
August 25, 2001	**Phelon.c**	**An IRC bot that executes raw commands.**
August 24, 2001	Alsou.c	Exploit for the Sendmail Debugger Arbitrary Code Execution vulnerability.
August 24, 2001	Xp.tar.gz	Exploit for the Sendmail Debugger Arbitrary Code Execution vulnerability.
August 22, 2001	**Killme.pl**	**Perl script which exploits the AOLServer Long Authentication String Remote Denial of Service vulnerability.**

Trends

Probes/Scans:

- **There has been an increase in scans of port 23 probing for the Multiple Vendor TelnetD vulnerability. (For more information, see the Multiple Vendor Telnetd Buffer Overflow vulnerability described in CyberNotes 2001-15 [July 30, 2001] located at http://www.nipc.gov/cybernotes/2001/cyberissue2001-15.pdf.)**
- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- **Recently, the cyber security community received numerous reports of intruders using the buffer overflow vulnerability in the Telnet daemon program. For more information, see NIPC ASSESSMENT 01-019, available at: http://www.nipc.gov/warnings/assessments/2001/01-019.htm. This vulnerability has the potential to impact the victim by allowing an intruder to copy, delete, or execute any program on the victim's system. A new worm called "x.c," designed to exploit this vulnerability, has also been discovered.**
- **The CERT/CC has observed a significant increase in activity resulting in compromises of home user machines. Many home users do not keep their machines up to date with security patches and workarounds, do not run current anti-virus software, and do not exercise caution when handling e-mail attachments. Intruders know this, and we have seen a marked increase in intruders specifically targeting home users who have cable modem and DSL connections.**
- **A modified variant of the Code Red worm, called Code Blue has emerged. that launches attacks against an IP address (211.99.196.135) associated with the Web site of a Chinese network security provider. For more information, see the Virus Section.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

CodeBlue (Aliases: IISWorm_BlueCode, BlueCode, Code Blue): This is an Internet worm that targets websites by affecting Internet Information Servers (ISS). It spreads from website to websites by sending and executing its EXE file. The names of the worm files are: 'SVCHOST.EXE' and 'HTTPEXT.DLL'. The EXE file is a Win32 application (PE EXE file) written in Microsoft C++. The worm infects only machines that have the Microsoft IIS package and website contents installed. The worm application being run on these machine locates and infects remote websites (remote machines with installed IIS package): by using the Web Directory Traversal exploit, it sends a copy of itself to them and spawns it on the remote host. As a result the worm infects all vulnerable webservers that can be accessed from the current infected machine, and other infected servers spread the worm. It has a payload routine that from 10:00am till 11:00am global time performs DoS attacks on a computer located in China. When installing itself, the worm creates its copies (EXE and DLL) in the root of C: drive, C:\SVCHOST.EXE and C:\HTTPEXT.DLL. This EXE file is then registered in the Registry auto-run key:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run Domain Manager = C:\svchost.exe
The worm then creates and generates a C:\D.VBS script file, then looks for the INETINFO.EXE application and terminates it, if it is active. The VBS script program also looks for Indexing Service, Indexing Query, and printer mapping and removes them. As a result, the worm removes vulnerabilities that can be used (or were used) by other worms to infect the machine or/and by malicious users to break into the server. To spread, the worm runs 100 threads that scan randomly selected IP addresses and attack them. To attack victim machines, the worm uses the Web Directory Traversal exploit three times:

1. it tries to determine IIS directory on remote machine,
2. then sends request to remote machine to download the virus's DLL component (HTTPEXT.DLL file) from an infected host,
3. the last request is to copy that DLL file to the C: drive's root directory.

To upload the DLL file to the victim machine, the worm uses the "TFTP" command, and it activates a temporary TFTP server on the infected (current) machine to process the "get data" command from the victimized (remote) machine.

IRC/Theme.worm (mIRC Worm): This is an IRC worm that usually pretends to be a "Lara Croft" desktop theme file. (Another version masqueraded as a theme named "Mesut".) It urges the user to use the theme with: "Hi there!! Check out tiz Lara Croft desktop theme: Click on the Preview screen saver button, its the best i've ever seen." If the user selects the preview screen saver button, the malicious code activates, changes the desktop, and may add/change the following files:

- \mirc\script.ini (modified)
- windows\win.vbe
- windows\laracroft.theme
- windows\mesut.theme
- C:\test.bat

VBS/Cuerpo-A (Visual Basic Script Worm): This is a polymorphic e-mail-aware worm that uses Microsoft Outlook to replicate. The worm arrives in an e-mail message either with a blank subject or with a random subject taken from the subject of messages already in Outlook folders. The attached filename is random and has a double extension (for instance, "txt (9 Kbytes).vbs"). There are 16 space characters after "txt." The inclusion of the phrase "(9 Kbytes)" appears to be an attempt by the worm to fool users into thinking the attached file is 9 KB in size. When the attached file is opened, the worm creates several randomly named VBS and HTML files in the Windows System directory. The worm changes the registry key:

HKCU\Software\Microsoft\Internet Explorer\Start Page

so that it points to a dropped HTML file called BLANK.HTM. The file contains a reference to "www.freedonation.com." It searches for e-mail addresses using two methods. First it looks through Outlook's contacts and other folders. It then searches all local and network drives for files with extensions .TXT, .NA2, .WAB, .MBX, .DBX and .DAT. If a file with that extension is found, it is read and the worm extracts any string that appears to be an e-mail address. The worm also attempts to copy itself into C:\Recycled\rndmein.vbs and changes the Registry keys:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Rndmein
and
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\sn

so that it runs on Windows startup. The origin of this worm is an HTML page on a website. If the website is accessed with Internet Explorer, the following warning message is displayed: "Some software (ActiveX controls) on this page might be unsafe. It is recommended that you do not run it. Do you want to allow it to run?." If the user chooses "Yes," then the page creates a file Winstart.bat in the Windows directory that will run on Windows startup and drop a worm file called 'rndmein.vbs'.

VBS.Emin.A@mm (Visual Basic Script Worm): This is a worm that creates a randomly named script file in a random folder, e-mails itself and a .doc file from the computer to all the addresses in the Microsoft Outlook address book, and then restarts the computer. The script file that it created then attempts to delete all files on drive C.

VBS_MERLIN.C (Aliases: MERLIN, MERLIN.C, VBS/Merlin.C@mm) (Visual Basic Script Worm): This is a destructive, polymorphic, Visual Basic Script (VBS) virus that propagates via e-mail in Microsoft Outlook, via the Gnutella network, and via MIRC. It copies itself to local and network drives. Upon first execution, it creates 10,000 randomly named directories in the root directory Drive C:\. It creates a text file with the same name in each directory. The file contains the following message:

Empty spaces - what are we waiting for
Abandoned places - I guess we know the score
Does anybody know what we are looking for
Inside my heart is breaking
My make-up may be flaking
But my smile still stays on
Whatever happens I'll leave it all to chance
Does anybody know what we are living for
Outside the dawn is breaking
But inside in the dark I'm aching to be free
My soul is painted like the wings of butterflies
Memories of yesterday will grow but never die
I can fly - my friends
I have to find the will to carry on
cause the show must go on - I love you, eva!

It then deletes the REGEDIT.EXE file and attempts to download and execute a CIH.EXE file from http://fws.freewebspace.com. Three days after it has installed itself, it disables the Windows Desktop using the registry, and then overwrites the AUTOEXEC.BAT file with instructions to format the hard drive C:\ upon next boot up. It also deletes the USER.DAT and SYSTEM.DAT files and then restarts Windows.

W32.Abotus.Worm@m (Win32 Worm): This worm is written in Delphi. When executed, the worm attempts to reply to all messages in the inbox. For the worm to function, an active MAPI session is required. This means that a MAPI compliant e-mail program, such as Microsoft Outlook, must be open. If an e-mail message has multiple recipients, the worm will only reply to the first one. Also, if the worm has been executed with Microsoft Outlook running, all messages in the inbox will be marked as "read." The worm does not modify any files or registry keys. This also means that if the worm is executed twice, it will perform the same actions twice. The e-mail that the worm sends out will appear as follows:

Subject: About Us
Message: I have included a program which illustrates my opinion about things you wrote me a few days ago
(NOTE: Due to a bug in the viral code, this worm will most likely fail when it attempts to send out e-mail.)

The worm adds the string "SMTP:" in front of each e-mail address.

W32/Choke.d.worm (Win32 Worm): This worm spreads via Microsoft's MSN Messenger program. If MSN Messenger is not installed on the local system, the worm could install itself, but would fail to spread to others from that system. The filename is "UNTITLED.JPEG.EXE." When run, the worm does not appear to do anything. However, in the background it loads itself into memory (the process name displayed in the task list is JK), hooks MSN Messenger events, and creates a registry run key to load itself at startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\
Run\MSN Messenger "%WormPath%\UNTITLED.JPEG.exe"

Once running, the worm monitors all incoming messages and responds with a reply containing the text, "finally got a new pic! :-)" Attached to this message is the worm itself (UNTITLED.JPEG.exe).

W32/Magistr-B (Aliases: W32/Magistr.B@MM, I-Worm.Magistr.b.poly, PE_MAGISTR.B, W32.Magistr.39921@mm) (W32 Executable File Virus): This is a variant of W32/Magistr-A, a polymorphic Windows 32 executable file virus which spreads by infecting files and via e-mail. The virus searches the user's address book, mailboxes, and other files present on the computer for e-mail addresses. It specifically targets addresses from Outlook Express, Netscape Navigator, and Internet Mail and News. It then sends itself to these e-mail addresses using its own SMTP client. The e-mail messages that are sent have a randomly generated subject, body text and attached filename. The possible attached filename extensions are .COM, .BAT, .PIF and .EXE.

W97M.Astia.BR (Alias: W97M.Pand.A) (Word 97 Macro Virus): This is a Microsoft Word macro virus that infects document (.doc) and template (.dot) files. It also modifies the following Microsoft Word options:

It changes:
- User Name to "J1nt0"
- User Initials to "J1n"
- User Address to "STM133PDG"

It disables the following settings:
- Virus Protection
- Save Normal Prompt
- Confirm Conversions

Finally, in the registry key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion, it changes the value data of RegisteredOwner to "PandA" and the value data of RegisteredOrganization to "J1nt0 Here Now !, Sorry."

WM97/CopyMe-A (Word 97 Macro Virus): This is a Word macro virus that has two methods of infecting documents. If the document already contains a macro with a 'Document_Open' subroutine, then the virus will infect by inserting a 'CopyMe' subroutine into the existing module. If the document does not contain a suitable macro, then the virus will infect by the more normal route of creating its own (in this case, a 'ThisDocument' module).

WM97/Ethan-EJ (Word 97 Macro Virus): This is a member of the WM97/Ethan family. The virus creates the non-viral file C:\etha.___, which it uses to replicate. Whenever a document is closed, there is a 30% chance that the virus will change the File Summary information so that the Title = "John Bell," the Author = "EW/LN/CB" and Keywords = "Kett."

WM97/Hope-P (Word 97 Macro Virus): This is a Word macro virus. If the day is equal to the month (for instance, if it is the 5th of May), then this virus will use the Office Assistant to display a message. The message is titled "CheeChoong!!" and contains the text "Have a great CheeChoong...."

WM97/Myna-AW (Word 97 Macro Virus): This is a minor variant of WM97/Myna-J caused by the virus interacting with a user macro. The virus has no malicious payload.

WM97/Titch-K (Word 97 Macro Virus): This is a member of the WM97/Titch family; it has no malicious payload. It creates the non-viral file C:\arbind2000.tmp, which it uses during replication. This file will normally be deleted by the virus after use.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table starts with Trojans discussed in CyberNotes #2001-01, and items will be added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	**N/A**	**Current Issue**
Backdoor.Acropolis	N/A	CyberNotes-2001-04
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.G_Door	**N/A**	**Current Issue**
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Netbus.444051	N/A	CyberNotes-2001-04
Backdoor.NTHack	N/A	CyberNotes-2001-06
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.Quimera	N/A	CyberNotes-2001-06
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	**N/A**	**Current Issue**
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-JZ	N/A	CyberNotes-2001-02
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
BAT.Install.Trojan	N/A	CyberNotes-2001-04
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_DELWIN.D	N/A	CyberNotes-2001-05
BAT_EXITWIN.A	N/A	CyberNotes-2001-01

Trojan	Version	CyberNotes Issue #
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	II	CyberNotes-2001-16
DLer20.PWSTEAL	N/A	CyberNotes-2001-05
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Flor	N/A	CyberNotes-2001-02
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
HackTack	**N/A**	**Current Issue**
HardLock.618	N/A	CyberNotes-2001-04
IRC/FinalBot	**N/A**	**Current Issue**
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Seeker.B	**N/A**	**Current Issue**
JS.StartPage	N/A	CyberNotes-2001-07
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	**2.1.28**	**Current Issue**
PHP/Sysbat	N/A	CyberNotes-2001-02
PIF_LYS	N/A	CyberNotes-2001-02
PWSteal.Coced240b.Tro	N/A	CyberNotes-2001-04
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
StealVXS	N/A	CyberNotes-2001-17
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/KillCMOS-E	N/A	CyberNotes-2001-01
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_AOL_EPEX	N/A	CyberNotes-2001-01
TROJ_AOLWAR.B	N/A	CyberNotes-2001-01
TROJ_AOLWAR.C	N/A	CyberNotes-2001-01
TROJ_APOST.A	**N/A**	**Current Issue**
TROJ_APS.216576	N/A	CyberNotes-2001-03
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_AZPR	N/A	CyberNotes-2001-01
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BAT2EXEC	N/A	CyberNotes-2001-01
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11
TROJ_BKDOOR.GQ	N/A	CyberNotes-2001-01
TROJ_BUSTERS	N/A	CyberNotes-2001-04
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
TROJ_CAINABEL151	1.51	CyberNotes-2001-06
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DARKFTP	N/A	CyberNotes-2001-03
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-04
TROJ_DUNPWS.CL	N/A	CyberNotes-2001-05
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FIX.36864	N/A	CyberNotes-2001-03
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_GLACE.A	N/A	CyberNotes-2001-01
TROJ_GNUTELMAN.A	N/A	CyberNotes-2001-05
TROJ_GOBLIN.A	N/A	CyberNotes-2001-03
TROJ_GTMINESXF.A	N/A	CyberNotes-2001-02
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_HERMES	N/A	CyberNotes-2001-03
TROJ_HFN	N/A	CyberNotes-2001-03
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_ICQCRASH	N/A	CyberNotes-2001-02
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_IF	N/A	CyberNotes-2001-05
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_INVALID.A	**N/A**	**Current Issue**
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JOINER.15	N/A	CyberNotes-2001-02
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE	N/A	CyberNotes-2001-04
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MYBABYPIC.A	N/A	CyberNotes-2001-05
TROJ_NAKEDWIFE	N/A	CyberNotes-2001-05
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NAVIDAD.E	N/A	CyberNotes-2001-01
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PARODY	N/A	CyberNotes-2001-05
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PORTSCAN	N/A	CyberNotes-2001-03
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_Q2001	N/A	CyberNotes-2001-06
TROJ_QZAP.1026	N/A	CyberNotes-2001-01
TROJ_RUNNER.B	N/A	CyberNotes-2001-03
TROJ_RUX.30	N/A	CyberNotes-2001-03

Trojan	Version	CyberNotes Issue #
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	**N/A**	**Current Issue**
TROJ_SUB7.21.E	2.1	CyberNotes-2001-05
TROJ_SUB7.22.D	.22	CyberNotes-2001-06
TROJ_SUB7.401315	N/A	CyberNotes-2001-01
TROJ_SUB7.MUIE	N/A	CyberNotes-2001-01
TROJ_SUB7.V20	2.0	CyberNotes-2001-02
TROJ_SUB722	2.2	CyberNotes-2001-06
TROJ_SUB722_SIN	N/A	CyberNotes-2001-06
TROJ_SUB7DRPR.B	N/A	CyberNotes-2001-01
TROJ_SUB7DRPR.C	N/A	CyberNotes-2001-03
TROJ_TPS	N/A	CyberNotes-2001-05
TROJ_TWEAK	N/A	CyberNotes-2001-02
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WEBCRACK	N/A	CyberNotes-2001-02
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
TROJ_ZERAF.A	**N/A**	**Current Issue**
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17
Trojan.JS.Cover	**N/A**	**Current Issue**
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.MircAbuser	N/A	CyberNotes-2001-04
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	**N/A**	**Current Issue**
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.RASDialer	N/A	CyberNotes-2001-06
Trojan.Sheehy	N/A	CyberNotes-2001-05
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Cute.A	N/A	CyberNotes-2001-05
VBS.Delete.Trojan	N/A	CyberNotes-2001-04
VBS.Fiber.C	**N/A**	**Current Issue**
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	**N/A**	**Current Issue**
VBS.Trojan.Lariara	**N/A**	**Current Issue**
VBS.Trojan.Noob	N/A	CyberNotes-2001-04
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09

Trojan	Version	CyberNotes Issue #
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BatmanTroj	N/A	CyberNotes-2001-04
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
Y3K Rat	1.6	CyberNotes-2001-11

Asylum (Alias: Backdoor.Asylum): This is a backdoor Trojan that works on Windows 9x/ME, NT/2000. The backdoor is located in the Windows directory and called 'winmp32.exe'. When run, it installs itself and sends a notification to the author about the infected machine using ICQ web interface. The service runs on TCP port 81 and is accessible from anywhere if the machine has a direct Internet connection.

Backdoor.G_Door (Alias: Backdoor.G_Door.c): Once activated, this backdoor Trojan inserts itself into the system so that it runs when Window starts, hooks the text-file viewing functionality, and gives the malicious user unrestricted remote control over the system. This Trojan has its own SMTP engine, which allows the malicious user to send e-mail without using the victim's e-mail program.

Backdoor.Way: This is a backdoor Trojan horse that allows unauthorized access to a compromised computer. When run, it first makes several copies of itself in the following locations:

- \%System%\Notepad.exe
- \%System%\msgsvc.exe
  (NOTE: %System% is a variable. The Trojan locates the \System folder (by default, on a Windows 95/98/Me computer this is C:\Windows\System) and copies itself to that location.)

These files are created with the "Hidden" and "System" attributes to hide them from the victim. Next, in the registry key:

HKEY_LOCAL_MACHINE\Software\Classes\txtfile\shell\open\command

it changes the Value data of the (Default) value from "C:\Windows\Notepad.exe %1" to "C:\Windows\System\Notepad.exe %1." This ensures that the Trojan file Notepad.exe is run instead of the real Notepad program whenever you open a .txt file. Finally, It adds the value "Msgtask C:\Windows\System\msgsvc.exe" to the key:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

This ensures that the Trojan is run every time the victim starts Windows.

HackTack (Alias: Backdoor.HackTack): This is a backdoor that allows a remote malicious user to take over a victim's machine. When run, the backdoor copies itself to the Windows directory as 'CfgWiz32.exe'. It adds a key to the registry in '[HKLM]\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' called 'Configuration Wizard' that points to the backdoor program in the Windows directory. This way the backdoor will be started whenever Windows boots up. When a machine has this backdoor any malicious user can connect to it with the HackTack client.

IRC/FinalBot (Alias: Trojan.Win32.JavaKiller (AVP): This is an elaborate zombie bot Trojan which enables others to remotely control a Windows system by sending commands via Internet Relay Chat. The main executable is a self-extracting archive (726,528 bytes) which contains 39 other files. When run, a crack searching program is displayed and the files are extracted. The .INI files contain instructions for the dropped mIRC client program, RUNDLLS.EXE, to act as a server. The Trojan uses registry keys to store variable information. The following registry keys are also created:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run\startwindowskeyuser=
HKLM\Software\Microsoft\Windows\CurrentVersion/RunServices\startwindowskeyuser=rundle2.exe

Phoenix (2.1.28): Once executed, this Trojan will place two server files into the victim's machine; it will then run in stealth mode and listen on port 7410 tcp. This Trojan possibly originates from South America. It lacks certain features found in other Trojans, but the client has an effective graphical user interface, which may increase its popularity.

Trojan.JS.Cover (Alias: Trojan.Magnatta): This Trojan arrives as a .html file. When opened, it displays garbage characters in the Web browser window. It exploits the ActiveX to modify the browser's home page. One variant of this Trojan prevents the victim from accessing the browser's Internet settings, making it difficult to change the browser's home page back to its previous setting.

JS.Seeker.B (Aliases: Troj/JetHome-B, JS/Seeker.gen, JS.Trojan.Seeker.b): This is a Windows Scripting Host (WSH) file which modifies Internet Explorer settings. When executed, this Trojan horse is usually copied to the Windows \StartUp folder as the file "run.hta." This ensures that it runs when Windows starts. It creates and then executes the registry import file C:\Windows\Homereg111.reg. When executed, it modifies Internet Explorer settings by making the following changes to the Windows registry:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\

it modifies the values:

Search Bar
Default_Search_URL
Search Page

so that they all point to a Web page that displays links to gambling, adult, and other sites. In the key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Search\

it modifies the value, "SearchAssistant," so that it points to the previously mentioned Web page. The script also creates a "favorite link" titled "Search The Web" which links to the same Web page.

Trojan.Pounds (Alias: Trojan.Error): This Trojan horse copies itself into the C:\Windows\System folder and configures a registry key so that it runs when Window starts. When it is run, it displays a message that a fatal error has occurred. It then displays a window with the following title: "Error - - - S#########ER." This window occasionally moves around the screen by itself. The screen also blacks out and then returns to normal. Eventually the mouse is limited to moving only within the displayed window.

TROJ_APOST.A (Aliases: APOST.A, I-Worm.Readme, READ.ME.A, W32.APOST-A): This Trojan/worm has been reported in the wild. It copies itself to all local drives of an infected system. It propagates via Microsoft Outlook by e-mailing itself as an attachment to all addresses listed in the infected user's address book. It sends e-mail four times to each address. It arrives in an e-mail with the subject line: "As per your request!" with the attachment "README.EXE." It does not have a destructive payload.

TROJ_INVALID.A (Alias: Win32.Invalid@mm): This Trojan is a mass-mailing Trojan/worm that arrives in an e-mail, purporting to originate from support@microsoft.com. The e-mail has the subject line "Invalid SSL Certificate." The e-mail body reads as follows:

> Hello,
> Microsoft Corporation announced that an invalid SSL certificate that web sites use is required to be installed on the user computer to use the HTTP protocol. During the installation, the certificate causes a buffer overrun in Microsoft Internet Explorer and by that allows attackers to get access to your computer. The SSL protocol is used by many companies that require credit card or personal information so, there is a high possibility that you have this certificate installed. To avoid of being attacked by hackers, please download and install the attached patch. It is strongly recommended to install it because almost all users have this certificate installed without their knowledge.
> Have a nice day,

An attachment to the message is called "SSLPATCH.EXE." Upon execution, the attachment searches for *.ht* in the My Documents folder. If found, it searches for the string "mailto:," obtains the e-mail address, and sends a copy of itself to that address. If no Internet connection is available, it corrupts .EXE files.

TROJ_SPYBOY.A (Aliases: SPYBOY, SPYBOY.A, TROJ_SPYBOY.B, IRC-Worm.SpyBoy): This multi-platform Trojan program propagates via mIRC. It has the following three components:

- IRC script
- .COM file
- An infected .VXD file

It arrives via IRC as BOY95.COM and infects the WIN32.VXD file in the Windows System folder. The infected system file then drops an IRC script in the C:\MIRC folder. The IRC Script component sends the COM file component, which is the BOY95.COM file, to any user that joins the same channel as the

infected user. It ignores users who send out messages with the following text strings in the infected channel: “boy95, LittleBoy, LBV, infect.” The IRC component of the worm contains the following text strings: “Little Boy Virus (Y2K Version) The Spy.” The .COM File component of the worm usually arrives as BOY95.COM. It opens the MS-DOS.SYS file and then finds the default Windows folder. Thereafter, it appends the string, ‘\SYSTEM’ to get to the Windows System directory where it searches for a VWIN32.VXD file. It then inserts itself in the VWIN32.VXD file. The .VXD component, which is the infected VWIN32.VXD, is a 16-bit component of Windows. It is a monolithic driver that contains several other drivers needed to run a system. Once infected with the worm, it drops an IRC.INI file in the C:\MIRC folder and a copy of the .COM component of the worm, BOY95.COM. In some instances, the worm fails to drop the .COM file. The VXD and the .COM file components of the worm contain the following text strings: “Little Boy Virus$The Spy$was here! :p$.”

TROJ_ZERAF.A: This is a destructive Trojan that deletes .EXE and .SYS files in an infected user's computer and causes an error in the Windows registry. It deletes component files such as HIMEM.SYS, RUNDLL.EXE, and COMMAND.COM. Therefore, an infected system can be restored only by reinstalling Windows.

VBS.Fiber.C: This is a variant of the VBS.Fiber.A Visual Basic Script (VBS) Trojan horse. It copies itself into the \Windows\System folder as VBS.Lava.vbs and modifies the registry so that this file is executed when Windows starts. If the current minute is :15, then the script's payload is activated as follows: A message is displayed that indicates how many times the script has been run and how many times you have been notified of its presence (but due to a bug, it does not show the number of notifications). It attempts to configure the registry so that the script is executed any time that an .htm or html file is opened on the computer.

VBS.Trojan.Icon: This is a Trojan horse that modifies the Windows registry. The modification to the registry causes HTML files to have a different icon from the default one. This Trojan has no other payload.

VBS.Trojan.Lariara: This is a Trojan horse that is written in the Visual Basic Scripting (VBS) language. When executed, the Trojan copies itself to the Windows startup folder so that it is executed each time that Windows is started. However, this only works under Windows 9x if the language is Spanish. If this Trojan is executed on the 22nd of October, it displays some message boxes over 1000 times. The payload works on all Windows systems.